REMARKS

This reply is responsive to the Office Action mailed on June 12, 2006. Claims 1-22 are pending in the application. Reconsideration in light of the following remarks is requested.

I. Rejection under 35 U.S.C. § 103

A. Carswell in view of Touboul

Claims 1-5 and 9-22 stand rejected under 35 U.S.C. § 103(a) as being obvious over Carswell et al. (U.S. Patent No. 5,365,591, issued November 15, 1994) in view of Touboul (U.S. Patent No. 5,978,579, issued July 18, 2000). Applicants respectfully disagree.

Carswell discloses that a secure cryptographic logic arrangement immediately halts the processing of its internal processors upon detection of a single fault. The cryptographic logic arrangement has an arithmetic logic unit, permuter, and a non-linear combiner. A total self-checking controller monitors each of the arithmetic logic unit, permuter, and non-linear combiner to determine whether a fault has occurred in any one of its internal processors. The total self-checking controller employs a scheme of transmitting a pseudorandom signal to each of the internal processors and compares a phase of the pseudorandom signal received back from each of the internal processors to determine whether a fault exists. (Carswell, Abstract)

Touboul discloses a system protects a computer from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the

Downloadable to determine if the security policy has been violated. The Downloadable may include a Java.TM. applet, an ActiveX.TM. control, a JavaScript.TM. script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, or a specific security policy to be applied based on the client or the group to which the client belongs. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components. Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable. (Touboul, Abstract)

The Examiner's attention is directed to the fact that Carswell and Touboul fail to disclose: a dual processor device that includes a host processor coupled to a secure processor where the secure processor decrypts the message **and** authenticates the message.

The present invention, in one embodiment, uses a secure processor operating with a host processor to perform a unitary decrypt authenticate operation. The host processor receives encrypted messages that include authentication information. The host processor must submit each message to the secure processor. The secure processor then decrypts and authenticates the message. If authentication is not successful, the secure processor does not return the fully decrypted message back to the host. In a preferred embodiment, the host will receive no part of the message upon failure. (Application, page 4, lines 9-15)

In contrast, neither Carswell nor Touboul teaches that a secure processor decrypts and authenticates a message. The Examiner concedes that Carswell fails to teach the use of authentication. Applicant further submits that Carswell does not teach, disclose, or suggest the use of a secure processor to authenticate a message. There is no mention of authentication anywhere in the Touboul reference. In addition, Touboul does not teach, disclose, or suggest the use of a secure processor to perform any of its teachings. Hence, there would have been no motivation to combine Carswell with Touboul even if it could be argued that Touboul teaches authentication. As such, the combination of Carswell and Touboul fails to establish a prima facie case of obviousness.

Therefore in view of the above, independent claims 1, 15, and 22 are patentable over Song. As such, claims 2-5, 9-14, and 16-22 are patentable at least by virtue of depending from their respective base claims. Applicants respectfully request withdrawal of the rejection.

B. Carswell in view of Atkinson

Claims 1-5 and 9-22 stand rejected under 35 U.S.C. § 103(a) as being obvious over Carswell et al. (U.S. Patent No. 5,365,591, issued November 15, 1994) in view of

Atkinson (U.S. Patent No. 5,892,904, issued April 6, 1999). Applicants respectfully disagree.

Carswell discloses that a secure cryptographic logic arrangement immediately halts the processing of its internal processors upon detection of a single fault. The cryptographic logic arrangement has an arithmetic logic unit, permuter, and a non-linear combiner. A total self-checking controller monitors each of the arithmetic logic unit, permuter, and non-linear combiner to determine whether a fault has occurred in any one of its internal processors. The total self-checking controller employs a scheme of transmitting a pseudorandom signal to each of the internal processors and compares a phase of the pseudorandom signal received back from each of the internal processors to determine whether a fault exists. (Carswell, Abstract)

Atkinson discloses that a certification or signing method ensures the authenticity and integrity of a computer program, an executable file, or code received over a computer network. The method is used by a publisher or distributor to "sign" an executable file so it can be transmitted with confidence to a recipient over an open network like the Internet. The executable file may be of any executable form, including an executable or portable executable .exe file format, a .cab cabinet file format, an .ocx object control format, or a Java class file. The code signing method assures the recipient of the identity of the publisher as the source of file (i.e., its authenticity) and that the file has not been modified after being transmitted by the publisher (i.e., the integrity of the file). As a result, the code signing method allows an executable file to be transmitted over open computer networks like the Internet with increased certainty in the identity of the source of the file and minimized risk of contracting a computer virus or other malicious executable computer files. (Atkinson, Abstract)

The Examiner's attention is directed to the fact that Carswell and Atkinson fail to disclose: a dual processor device that includes a host processor coupled to a secure processor where the secure processor decrypts the message **and** authenticates the message.

The present invention, in one embodiment, uses a secure processor operating with a host processor to perform a unitary decrypt authenticate operation. The host processor receives encrypted messages that include authentication information. The host processor must submit each message to the secure processor. The secure processor then decrypts and authenticates the message. If authentication is not successful, the secure processor does not return the fully decrypted message back to the host. In a preferred embodiment, the host will receive no part of the message upon failure. (Application, page 4, lines 9-15)

In contrast, neither Carswell nor Atkinson teaches that a secure processor decrypts and authenticates a message. The Examiner concedes that Carswell fails to teach the use of authentication. Applicant further submits that Carswell does not teach, disclose, or suggest the use of a secure processor to authenticate a message. Although Atkinson does disclose the use of authentication, Atkinson, like Carswell, also fails to teach, disclose, or suggest the use of a secure processor to authenticate a message. If the Examiner is arguing that the secure cryptographic logic arrangement of Carswell and the authentication disclosed by Atkinson reads on the claims of the present invention, that would constitute improper hindsight reasoning since neither Atkinson nor Carswell discloses the use of a secure processor to authenticate a message. In addition, since Atkinson does not contemplate the use of a secure processor in providing authentication, there would be no motivation to combine Carswell with Atkinson. As such, the combination of Carswell and Atkinson fails to establish a prima facie case of obviousness.

Therefore in view of the above, independent claims 1, 15, and 22 are patentable over Carswell and Atkinson. As such, claims 2-5, 9-14, and 16-22 are patentable at least by virtue of depending from their respective base claims. Applicants respectfully request withdrawal of the rejection.

C. Carswell and Touboul in view of Miller

Claims 6-8 stand rejected under U.S.C. § 103(a) as being obvious over Carswell and Touboul in view of Miller (U.S. Patent No. 5,402,474, issued March 28, 1995). Applicant respectfully disagrees.

As argued above in Section I. A., Carswell and Touboul fail to disclose a dual processor device that includes a host processor coupled to a secure processor where the secure processor decrypts the message **and** authenticates the message. The Examiner concedes that Carswell and Touboul fail to teach coupling a provisioning server, a billing host and a customer service representative center with the cable telephony network. In order to cure the Examiner's perceived deficiency of Carswell and Touboul, the Examiner cites Miller.

Miller discloses providing a programmable interface between a workstation and an archive server to automatically store information derived from a telephone transaction.

The archive server stores a data base of records having a plurality of category fields for information derived from the telephone transaction. A host access table stored in a memory in the workstation, contains programmable commands. An interface program stored in the workstation memory executes the commands in the host access table, to perform interfacing functions between a host computer and the telephone network and to perform interfacing functions between the workstation and the archive server. (Miller, Abstract)

As stated above, Carswell and Touboul fail to disclose fail to disclose a dual processor device that includes a host processor coupled to a secure processor where the secure processor decrypts the message **and** authenticates the message. Carswell and Touboul in combination with Miller fails to cure this deficiency.

As such, Applicant submits that claims 6-8, are patentable in view of the above arguments and at least by virtue of depending from their respective base claims. Therefore, Applicant respectfully requests withdrawal of the rejection.

D. Carswell and Atkinson in view of Miller

Claims 6-8 stand rejected under U.S.C. § 103(a) as being obvious over Carswell and Atkinson in view of Miller (U.S. Patent No. 5,402,474, issued March 28, 1995). Applicant respectfully disagrees.

As argued above in Section I. B., Carswell and Atkinson fail to disclose a dual processor device that includes a host processor coupled to a secure processor where the secure processor decrypts the message **and** authenticates the message. The Examiner concedes that Carswell and Atkinson fail to teach coupling a provisioning server, a billing host and a customer service representative center with the cable telephony network. In order to cure the Examiner's perceived deficiency of Carswell and Atkinson, the Examiner cites Miller.

Miller discloses providing a programmable interface between a workstation and an archive server to automatically store information derived from a telephone transaction. The archive server stores a data base of records having a plurality of category fields for information derived from the telephone transaction. A host access table stored in a memory in the workstation, contains programmable commands. An interface program stored in the workstation memory executes the commands in the host access table, to perform interfacing functions between a host computer and the telephone network and to perform interfacing functions between the workstation and the archive server. (Miller, Abstract)

As stated above, Carswell and Atkinson fail to disclose fail to disclose a dual processor device that includes a host processor coupled to a secure processor where the secure processor decrypts the message **and** authenticates the message. Carswell and Atkinson in combination with Miller fails to cure this deficiency.

As such, Applicant submits that claims 6-8, are patentable in view of the above arguments and at least by virtue of depending from their respective base claims. Therefore, Applicant respectfully requests withdrawal of the rejection.

Conclusion

Having fully responded to the Office action, the application is believed to be in condition for allowance. Should any issues arise that prevent early allowance of the above application, the Examiner is invited contact the undersigned to resolve such issues.

To the extent an extension of time is needed for consideration of this response, Applicants hereby request such extension and, the Commissioner is hereby authorized to charge deposit account number 502117 for any fees associated therewith.

Date: 3/28/2007

Respectfully submitted,

By: /Thomas Bethea, Jr./
Thomas Bethea, Jr.
Reg. No.: 53,987

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1850